AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes a change to Fig. 8. The sheet, which includes Fig. 8, replaces the original sheet for Fig. 8. In Fig. 8, an arrow that erroneously pointed from element 820 to element 845 has been changed to point from element 830 to element 835. Also, the text in the box of element 820 has been changed by replacing "private" with "public".

REMARKS

Claims 1-5, 8-16, 19-25, 28-34, 37-43, 46-52 and 55-63 are pending in the present application. In the above amendments, claim 9 has been amended.

Applicant respectfully responds to this Office Action.

Objections to the Specification

The specification was objected to a failing to provide proper antecedent basis for the subject matter of claims 9-12, 28-30, 46-48 and 62-63. Applicants have amended claim 9 to remove reference "for the terminal" in reference to the private key. Unlike claim 9, claims 28, 46 and 62 do not have the reference "for the terminal" in reference to the private key. Further, FIG. 8 has been amended to correct a pointing error between step 830 and step 835, and to correct the text in the box for element 820. According to the specification, "FIG. 8 shows another example method 800 for provisioning of BAK in a terminal when a content provider possesses a private key. Method 800 begins when a content provider distributes a public key corresponding to the private key (805). **After receiving the public key (810), UIM of the terminal encrypts RK using the public key (820).** The RK would be stored in a secure memory such as SUMU 434. **The encrypted RK is sent to a content provider (830). The content provider receives the encrypted RK (835) and decrypts RK using the private key (845).**" See, page 15, line 29 through page 16, line 3. The drawing amendment is supported by the highlighted text quoted above. The specification clearly recites that the terminal encrypts the secret key (RK) using the public key in step 820. The next step is 830 (sending from the terminal), which is followed by step 835. The over-the-air exchange of keys is disclosed in the specification at page 10, line 7. Accordingly, the objection to the specification, as failing to provide proper antecedent basis for the subject matter of claims 9-12, 28-30, 46-48 and 62-63, should be withdrawn.

Claim Rejections – 35 USC § 112

Claims 9-12, 19-21, 28-30, 37-39, 46-48, 55-57 and 62-63 have been rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Regarding claims 9-12, 28-30, 46-48 and 62-63, claim 9 and FIG. 8 have been amended to

correct the corresponding disclosure failures, as discussed above. Regarding claims 19-21, 37-39 and 55-57, the receiving and decrypting steps at the content provider are disclosed in the specification at page 16, lines 1-3, and by FIG. 8, steps 835 and 845. Accordingly, the rejections of claims 9-12, 19-21, 28-30, 37-39, 46-48, 55-57 and 62-63, as failing to comply with the written description requirement, should be withdrawn.

Claim Rejections – 35 USC § 103

Claims 1-5, 8, 13-16, 22-25, 31-34, 40-43, 49-52 and 58-61 have been rejected under 35 U.S.C. §103 as being unpatentable over U.S. Patent Re. 33,189 to Lee et al., in view of U.S. Patent No. 5,870,474 to Wasilewski et al., further in view of U.S. Patent No. 6,424,947 to Tsuria et al.,and further in view of U.S. Patent No. 5,878,141 to Daly. Claims 9-12, 19-21, 28-30, 37-39, 46-48, 55-57 and 62-63 have been rejected under 35 U.S.C. §103 as being unpatentable over U.S. Patent Re. 33,189 to Lee et al., in view of U.S. Patent No. 5,870,474 to Wasilewski et al., and further in view of U.S. Patent No. 6,424,947 to Tsuria et al.

The rejection of claim 1 as allegedly unpatentable over the Lee, Wasilewski, Tsuria and Daly patents is respectfully traversed. Claim 1 recites "distributing, over-the-air from the terminal, a public key corresponding to the private key" stored by the terminal. This paragraph of the claim recites, at most, five limitations: 1) distributing; 2) over the air; 3) from the terminal; 4) a public key; and 5) corresponding to a private key. The Examiner cites the disclosure of four different patents for teaching portions of this feature. More specifically, the Examiner asserts that the Lee patent discloses "distributing a key (user ID, col. 3, lines 28-42)", that the Wasilewski patent teaches there "is a private key stored in a set top unit (col. 8, line 44-47) where the second level key is encrypted with the public key which corresponds with the intended set top unit (col. 8, lines 39-41)", that the Tsuria patent "teaches a system where a wireless subscriber unit receives television transmissions over they air (RF link) (col. 9, line 35-48) to eliminate the need for a physical cable connection", and that Daly patent teaches "a wireless distribution structure is anticipated (col. 9, lines 35-39)", and teaches "exchanging digital certificates between the STB (set top box) and the head end (col. 15, line 10-26)". See, Office Action, page 9, lines 4-5, 11-13, and page 10, lines 1-3 and 13-16. Further, the Examiner acknowledges that the Lee patent, as modified by the Wasilewski and Tsuria patents, fails to

disclose "distributing the public key over the air from the terminal". See, Office Action, page 10, line 10. This corresponds to limitations 1-4. Thus, the Examiner is asserting that the Lee patent teaches limitations 1, 3 and 5, the Wasilewski patent teaches limitations 3, 4 and 5, the Tsuria patent teaches limitations 2 and 3, and the Daly patent teaches limitations 1, 3, 4 5 (the Daly patent's disclosure related to 2 is extremely vague). The Daly patent, however, is not asserted as disclosing any features recited in the remaining paragraphs of claim 1.

Regarding reasons for combining the cited patents, the Examiner concludes, "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to utilize a public/private key pair as a replacement for the user ID and distribute a public key (to service providers) from the terminal (set top box) and from a directory. One of ordinary skill in the art would have been motivated to perform such a modification because **it obviates the need to securely transfer an endless hierarchy of keys and allows multiple service providers to communicate with the set top unit**, as taught by Wasilewski." Further, the Examiner concludes, "it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Lee to use a wireless terminal and therefore, distribute the public key from the terminal (once it is generated, as taught by Wasilewsky) over the air and to receive the secret key over the air (television communications). One of ordinary skill in the art would have been motivated to perform such a modification to **gain the known benefits of wireless computing devices, such as the elimination of direct cable connections**, as taught by Tsuria". The Examiner further concludes, "it would have been obvious to purchase programming by exchanging public keys between the set top unit and the head end and then use the exchanged keys for communication, as taught by Daly. One of ordinary skill in the art would have been motivated to perform such a modification **to perform interactive program ordering of services from the head end**, as taught by Daly". See, Office Action, page 4, lines 6-8; page 9, lines 15-21; page 10, lines 3-9; and line 19 - page 11, line 1.

In analyzing the issue of obviousness, it is necessary to guard against slipping into the use of hindsight, and to resist the temptation to read into the prior art the teachings of the invention at issue. See, Graham v. John Deere Co., 383 U.S. 1, 36 (1966). Applicants assert that the Examiner has use hindsight analysis in analyzing claim 1. Applicants assert that the Examiner searched for each feature, and kept combining prior art patents until a sufficient

number of patent were aggregated to identify the limitations recited in the first paragraph of claim 1, which paragraph has a length of only two lines. Further, the Examiner's reasons for combining the patents are merely conclusionary statement of obviousness. For example, the Examiner merely concludes, "one of ordinary skill in the art would have been motivated to perform such a modification **to perform interactive program ordering of services from the head end**, as taught by Daly." In addition, other conclusions fail to consider the negative aspects of the asserted combinations. For example, the Examiner concludes, "One of ordinary skill in the art would have been motivated to perform such a modification to **gain the known benefits of wireless computing devices, such as the elimination of direct cable connections**, as taught by Tsuria". However, the negative aspects of transmitting keys for encryption "over-the-air" are never addressed by the Examiner. The present invention recited by claim 1 satisfies a need for secure and efficient provisioning of a secret key to a sender and a recipient. See, specification, page 2, line 9-10.

Accordingly, the rejection of claim 1 as allegedly unpatentable over the Lee, Wasilewski, Tsuria and Daly patents should be withdrawn.

It is respectfully submitted that dependent claims 2-4 are at least allowable for the reasons given above in relation to independent claim 1.

Claims 5, 8, 13-16, 22-25, 31-34, 40-43, 49-52 and 58-61 are rejected by the combined teaching of the he Lee, Wasilewski, Tsuria and Daly patents. For reasons similar to the impermissible hindsight analysis discussed above with respect to claim 1, the rejections of claims 5, 8, 13-16, 22-25, 31-34, 40-43, 49-52, 58-59 and 62-63, as allegedly unpatentable over the Lee, Wasilewski, Tsuria and Daly patents, should be withdrawn.

The rejection of claim 60 as allegedly unpatentable over the Lee, Wasilewski, Tsuria and Daly patents is respectfully traversed. Claim 60 recites "distributing, over-the-air from the **User Identification Module**, a public key corresponding to the private key" stored by the User Identification Module. The Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. To establish a *prima facie* case of obviousness, the prior art references must teach or suggest all the claim limitations. See, MPEP § 2143. The Office Action fails to even mention the User Identification Module recited in claim 60. Accordingly, with

respect to claim 60, Applicants assert that the Examiner has failed to make a *prima facie* case of obviousness.

It is respectfully submitted that dependent claim 61 is at least allowable for the reasons given above in relation to independent claim 60.

The rejection of claim 9 as allegedly unpatentable over the Lee, Wasilewski, and Tsuria patents is respectfully traversed. Claim 9 recites "receiving, over-the-air at the terminal, a public key corresponding to a private key; encrypting the secret key at the terminal with the public key; sending, over-the-air from the terminal, the encrypted secret key; receiving the access key encrypted by the secret key at the terminal; and decrypting the access key ~~by~~ with the secret key at the terminal. The Examiner cites the disclosure of three different patents for teaching portions of these features. In analyzing the issue of obviousness, it is necessary to guard against slipping into use of hindsight, and to resist the temptation to read into the prior art the teachings of the invention at issue. Graham v. John Deere Co., 383 U.S. 1, 36 (1966). For reasons similar to those given above with respect to claim 1, Applicants assert that the Examiner has used hindsight analysis in analyzing claim 9. Accordingly, the rejection of claim 9 as allegedly unpatentable over the Lee, Wasilewski, and Tsuria patents should be withdrawn.

It is respectfully submitted that claims 10-12, 19-21, 28-30, 37-39, 46-48, 55-57 and 62-63 are at least allowable for the reasons given above in relation to independent claim 9.

Applicants incorporate into this Amendment, the "No Reasonable Expectation Of Success" argument presented in the prior Amendment of March 16, 2007. The essence of the Examiner's response was an assertion that "the entire system would not need to be replaced." See, Office Action, page 3, line 10.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **September 19, 2007**

By: / Won Tae C. Kim /
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502